Europ. J. Combinatorics (1998) **19**, 159–174

On the Existence of Cyclic and Pseudo-Cyclic MDS Codes

TATSUYA MARUTA

Conditions for the existence of pseudo-cyclic MDS codes of dimension k (especially $k \leq 5$) are studied. Existence tables for cyclic or pseudo-cyclic $[n, k]_q$-MDS codes are also given for $q \leq 64$, $k = 3, 4, 5$.

1. INTRODUCTION

We denote by F_q the Galois field of order $q = p^h$, p prime. An $[n, k]_q$-code means a linear code of length n and dimension k over F_q. An $[n, k]_q$-code with minimum (Hamming) distance d is called *maximum distance separable* (MDS) if $d = n - k + 1$. Note that the dual code of an MDS code is also MDS, see [10, Chapter 11]. Let α be a fixed non-zero element of F_q. A code C is *α-cyclic* if $(x_1, x_2, \ldots, x_n) \in C$ implies $(\alpha x_n, x_1, x_2, \ldots, x_{n-1}) \in C$. A code C is called *pseudo-cyclic* (or *semi-cyclic* [11]) if C is α-cyclic for some $\alpha \in F_q^*$, $F_q^* = F_q \setminus \{0\}$. Pseudo-cyclic codes were first introduced by E. R. Berlekamp [2] using the name of *constacyclic codes*. The dual code of an α-cyclic code is α^{-1}-cyclic. 1-cyclic codes are simply called *cyclic*.

One of the most popular classes of codes in algebraic coding theory are *Reed–Solomon* codes, which are cyclic MDS codes of length $q - 1$ over F_q. Our research problem is to find all n for which cyclic or pseudo-cyclic $[n, k]_q$-MDS codes exist for given k, q.

To avoid trivial cases we assume $q \geq k$ and $3 \leq k \leq n - 3$. It is well known that there exists a pseudo-cyclic $[n, k]_q$-MDS code if $q \equiv \pm 1 \bmod n$ or $n = p$ and that $(n, q) \neq 1$ implies $n = p$ [9, 11, 15, 16], where (n, q) stands for the greatest common divisor of n and q. We can construct cyclic $[n, k]_q$-MDS codes if $q \equiv 1 \bmod n$ or $n = p$ [1, 10]. For the case $q \equiv -1 \bmod n$, the following theorem is known.

THEOREM A ([15]). *When n divides $q + 1$, an α-cyclic $[n, k]_q$-MDS code exists iff either*

(1) *n is odd,*

(2) *n is even, q and k are odd, and α is a quadratic residue in F_q or*

(3) *q is odd, n and k are even, and α is a quadratic non-residue in F_q.*

Our aim is to find $[n, k]_q$-MDS codes with $q \not\equiv \pm 1 \bmod n$ and $n \neq p$. Hence we assume the following throughout this paper:

ASSUMPTION. $q \geq k$, $3 \leq k \leq n - 3$, $(n, q) = 1$ and $q \not\equiv \pm 1 \bmod n$.

In Section 2 we give some new results on pseudo-cyclic codes and pseudo-cyclic MDS codes. In Section 3 we survey known results on pseudo-cyclic MDS codes of dimension three. In Sections 4 and 5, necessary conditions for the existence of $[n, k]_q$-MDS codes are given for $k = 4, 5$, and sufficient conditions are also given for some small n. In the last section we give existence–non-existence tables of cyclic or pseudo-cyclic $[n, k]_q$-MDS codes for $q \leq 64$, $k = 3, 4, 5$.

0195-6698/98/020159 + 16 $25.00/0 ej970167

2. Pseudo-Cyclic Codes and Pseudo-Cyclic MDS Codes

We associate the vector $c = (c_0, c_1, \dots, c_{n-1}) \in F_q^n$ with the polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$. With this association an α-cyclic code C can be identified as an ideal of the ring $F_q[x]/(x^n - \alpha)$. Hence we can treat pseudo-cyclic codes similarly to cyclic ones.

Let C and C' be $[n, k]_q$-codes. C and C' are *equivalent* if there exists a monomial matrix M with entries in F_q such that C' coincides with $CM = \{cM \mid c \in C\}$.

LEMMA 2.1 ([12]). *Let C be an α-cyclic $[n, k]_q$-code. If there exists an element $\beta \in F_q$ with $\beta^n = \alpha$ (e.g. if $(n, q-1) = 1$), then there exists a cyclic $[n, k]_q$-code which is equivalent to C.*

LEMMA 2.2 ([12]). *Let η be an element of F_{q^d} with $\eta^n = \alpha$, $\alpha \in F_q^*$. Put $s = (n, \sum_{i=0}^{d-1} q^i)$ and $n = rs$. If $n | q^d - 1$ (i.e. n divides $q^d - 1$), then there exists an element β in F_q such that $\beta^r = \alpha$.*

For a given matrix T we denote by ${}^tT$ the transpose of T. The following theorem describes a parity check matrix for an α-cyclic code.

THEOREM B ([11]). *Let $g(x)$ be a polynomial of degree k in $F_q[x]$ dividing $x^n - \alpha$, $\alpha \in F_q^*$. Then C is an α-cyclic $[n, n-k]_q$-code with the generator polynomial $g(x)$ iff C is a code with a parity check matrix of the form $[{}^tP, {}^t(PT), {}^t(PT^2), \dots, {}^t(PT^{n-1})]$, where $P = (1, 0, \dots, 0)$ and T is the companion matrix of $g(x)$, i.e.*

$$T = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{k-1} \end{pmatrix} \quad \text{if } g(x) = \sum_{i=0}^{k} a_i x^i \text{ with } a_k = 1.$$

PROOF. We give a shorter elementary proof here rather than the original proof of [11]. Let C be an α-cyclic $[n, n-k]_q$-code with the generator polynomial $g(x)$. Let T be the companion matrix of $g(x)$. Since $g(T) = O$, we have $T^n = \alpha I_k$, where I_k is the identity matrix of size k and O is the zero matrix. Put $H = [{}^tP_0, {}^tP_1, \dots, {}^tP_{n-1}]$, $P_i = PT^i$, $P_0 = P = (1, 0, \dots, 0)$. $PT^n = \alpha P$ implies that H forms a parity check matrix of an α-cyclic $[n, n-k]_q$-code by [11, Theorem 2]. We show that H is a parity check matrix of C. Let G be the canonical generator matrix of C, i.e.

$$G = \begin{pmatrix} a_0 & a_1 & \dots & a_{k-1} & 1 & & \\ & a_0 & a_1 & \dots & a_{k-1} & 1 & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \\ & & & a_0 & a_1 & \dots & a_{k-1} & 1 \end{pmatrix},$$

where $g(x) = \sum_{i=0}^{k} a_i x^i$ with $a_k = 1$. Since $g(x)$ is the characteristic polynomial of T, we have $a_0 P + a_1 PT + \cdots + a_{k-1} PT^{k-1} + PT^k = P(T^k + a_{k-1}T^{k-1} + \cdots + a_1 T + a_0 I_k) = Pg(T) = O$, whence $G\,{}^tH = O$. This completes the proof. □

For an α^{-1}-cyclic $[n, k]_q$-code C, $\alpha \in F_q^*$, the generator polynomial $g(x)$ of the dual code $C^\perp$ is called the *check polynomial* of C. By Theorem B, C has a generator matrix of the form $[{}^tP, {}^t(PT), {}^t(PT^2), \dots, {}^t(PT^{n-1})]$,where $P = (1, 0, \dots, 0)$ and T is the companion matrix of $g(x)$. On the other hand, $g(x)$ can be written as $g(x) = \prod_{i=1}^{k}(x - \eta_i)$, $\eta_1, \dots, \eta_k \in K$, for some extension field K of F_q. Since $C^\perp$ corresponds to the ideal of $F_q/(x^n - \alpha)$ generated

by $g(x)$, $C^{\perp}$ has a parity check matrix of the form

$$\begin{pmatrix} 1 & \eta_1 & \dots & \eta_1^{n-1} \\ 1 & \eta_2 & \dots & \eta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \eta_k & \dots & \eta_k^{n-1} \end{pmatrix} \quad \text{with } \eta_i^n = \alpha \text{ for all } i.$$

Clearly, the F_{q^r}-span of an α-cyclic code over F_q is an α-cyclic code over F_{q^r}. Recall that every square submatrix of size k of a generator matrix G of an $[n, k]_q$-MDS code is non-singular and that every square submatrix of G' is non-singular when $G = [I_k, G']$, see [10]. Hence the F_{q^r}-span of an MDS code over F_q is an MDS code over F_{q^r}. These properties are frequently used in this paper.

LEMMA 2.3 ([12]). *If there exists no pseudo-cyclic $[s, k]_q$-MDS code and if s divides n, then there exists no pseudo-cyclic $[n, k]_q$-MDS code.*

LEMMA 2.4 ([12]). *Let C be a pseudo-cyclic $[n, k]_q$-code with the check polynomial $g(x)$. Let $g_1(x), g_2(x), \dots, g_s(x)$ be the irreducible factors of $g(x)$ over F_q. Put $d = \text{l.c.m.}\{\deg g_i(x); 1 \le i \le s\}$. If $(n, q^d - 1) \neq n$, then C has a codeword with weight two and hence C is not MDS.*

The following lemma is concerned with the factorization properties of the check polynomial of a pseudo-cyclic MDS code.

LEMMA 2.5. *Let C be a pseudo-cyclic $[n, k]_q$-MDS code with the check polynomial $g(x)$.*

(1) *If $g(x)$ has ℓ irreducible factors of degree $d \ge 2$ with $k = d\ell \ge \ell + 1$, then $n/u \le \ell$, where $u = (n, \frac{q^d-1}{q-1})$.*
(2) *If $g(x)$ has m linear factors and ℓ irreducible factors of degree $d \ge 2$ with $k = m + d\ell$, $1 \le \ell < k/d$, then $m \le (n, q-1) \le \ell$ for $d = 2$ with $m \ge 2$, or $d \ge 3$ and $1 \le (n, q-1) \le \ell + 1$ for $d = 2$, $m = 1$.*
(3) *If $g(x)$ has e_i irreducible factors of degree d_i, $i = 1, \dots, D$ with $k = \sum_{i=1}^{D} e_i d_i$, $1 < d_1 < d_2 < \cdots < d_D$, and if $(n, \prod_{i=1}^{D} \frac{q^{d_i}-1}{q-1}) > k$ and $\sum_{i=1}^{D}(n, q^{d_i} - 1) < n$ hold, then either $k \le 2^D - 1$ holds or there exists a prime number r dividing (n, d_i) with $r^2 | n$ for some i, $1 \le i \le D$.*

PROOF.

(1) Suppose that $g(x)$ divides $x^n - \alpha$, $\alpha \in F_q^*$. Let $u = (n, \frac{q^d-1}{q-1})$ and $n = uv$. By Lemma 2.4 v divides $q - 1$. Thus we have $x^n - \alpha = \prod_{i=1}^{v}(x^u - \beta\sigma^i)$ for some β, $\sigma \in F_q^*$ by Lemma 2.2. Let $f(x)$ be the product of all $(x^u - \beta\sigma^i)$ such that $(g(x), x^u - \beta\sigma^i) \neq 1$. If $v > \ell$ then $f(x)$ is a non-zero codeword of $C^{\perp}$ with weight at most $\ell + 1 \le k$, a contradiction.
(2) Since $g(x)$ has a linear factor, we may assume that C is cyclic by Lemma 2.1. Let $(n, q-1) = r$, $n = rs$. Clearly $r \ge m$. Let ρ be a primitve rth root of unity. Then we can write $x^n - 1 = \prod_{i=1}^{r}(x^s - \rho^i)$. Let J be a collection of j's such that $x^s - \rho^j$ has an irreducible factor of degree d in $g(x)$, $1 \le j \le r$. Let $x^r - a$ be the product of all linear factors in $x^n - 1$, $a \in F_q^*$. Put $h(x) = (x^r - a)\prod_{j \in J}(x^s - \rho^j)$. If $r \ge \ell + 1$, then $h(x)$ is a non-zero codeword of $C^{\perp}$ with weight at most $2(\ell + 1) = 2(k - m + d)/d \le k$ except for the case $d = 2$, $m = 1$, giving a contradiction. For the case when $d = 2$ and $m = 1$, we get a contradiction similarly if $r > \ell + 1$.

(3) Suppose $g(x)$ divides $x^n - \alpha$, $\alpha \in F_q^*$, and that there exists no prime r dividing (n, d_i) with $r^2 | n$ for any i, $1 \leq i \leq D$. Since $(n, \prod_{i=1}^{D} \frac{q^{d_i}-1}{q-1}) > k$, we may replace $(n, \prod_{i=1}^{D} \frac{q^{d_i}-1}{q-1})$ with n by Lemma 2.3. Put $n_i = (n, q^{d_i} - 1)$, $n = n_i n_i'$ and $m_i = (n_i', q-1)$. Suppose $m_i > 1$. Since m_i divides n_i, m_i^2 divides n. Taking a prime r dividing m_i, r divides $\sum_{i=0}^{d_j-1} q^{\ell}$ $(\equiv d_j \bmod r)$ for some j, whence r divides d_j, a contradiction. Hence $m_i = 1$ for any i, $1 \leq i \leq D$. It follows that there exists an element $\beta_i \in F_q$ with $\beta_i^{n_i'} = \alpha$. Let $f(x) = \prod_{i=1}^{D}(x^{n_i} - \beta_i)$. Since $g(x)$ divides $f(x)$ and $\deg f(x) = \sum_{i=1}^{D} n_i < n$, $f(x)$ is a non-zero codeword of $C^{\perp}$ with weight at most 2^D and hence $k \leq 2^D - 1$. □

COROLLARY 2.6. *Let C be a pseudo-cyclic $[n, k]_q$-MDS code with the check polynomial $g(x)$. If $g(x)$ is irreducible over F_q, then $\sum_{i=0}^{k-1} q^i \equiv 0 \bmod n$.*

COROLLARY 2.7. *Let C be a pseudo-cyclic $[n, k]_q$-MDS code with the check polynomial $g(x)$. If $g(x)$ has an irreducible factor of degree $k-1$ over F_q, then $\sum_{i=0}^{k-2} q^i \equiv 0 \bmod n$ and $(n, q-1) = 1$.*

LEMMA 2.8. *If $d = 2$ and $(n, q-1) = 2$ in Lemma 2.5(2), then $q \equiv 4t - 1 \bmod n = 8t$ for some integer t, and k is odd.*

PROOF. Since $d = (n, q-1) = 2$ implies $n | q^2 - 1$ and $\frac{n}{2} | q + 1$, we have $4 | n$. Since 4 does not divide $q - 1$, we have $4 | (n, q+1)$. Hence $n = 8t$ for some integer t. Since $4t | q + 1$ and $q \not\equiv -1 \bmod n$, we obtain $q \equiv 4t - 1 \bmod n = 8t$. By Theorem A, there does not exist a cyclic $[4t, k]_q$-MDS code if k is even. Hence k must be odd. □

THEOREM 2.9. *Let C_i be a cyclic $[n, n-k]_q$-MDS code with the generator polynomial $g_i(x)$ and with the minimum distance d_i, $i = 1, 2$.*

(i) If both $g_1(x)$ and $g_2(x)$ are irreducible over F_q and if $d_1, d_2 \geq 3$, then C_1 and C_2 are equivalent.

(ii) If each $g_i(x)$ has an irreducible factor of degree $k-1$ over F_q, $i = 1, 2$, and if $d_1, d_2 \geq 5$ with $k \geq 4$, or $d_1, d_2 \geq 3$ with $k = 3$, then C_1 and C_2 are equivalent.

PROOF.

(i) Suppose that both $g_1(x)$ and $g_2(x)$ are irreducible over F_q. Let $g_1(x) = \prod_{j=1}^{k}(x - \eta^{q^j})$ and $g_2(x) = \prod_{j=1}^{k}(x - \eta^{iq^j})$, $1 < i < n$, where η is a primitive nth root of unity. Put $s = (n, i)$, $n = sn'$. If $s > 1$, then $g_2(x)$ divides $x^{n'} - 1$, $n' < n$, whence C_2 has a codeword with weight two, a contradiction. Hence $s = 1$, which implies that $\{1, 2, \ldots, n\} \to \{i, 2i, \ldots, ni\}$ is a permutation under modulo n. C_2 has a parity check matrix whose columns consist of

$$\{{}^t(\eta^{ij}, \eta^{ijq}, \ldots, \eta^{ijq^{k-1}}); j = 1, 2, \ldots, n\} = \{{}^t(\eta^{j}, \eta^{jq}, \ldots, \eta^{jq^{k-1}}); j = 1, 2, \ldots, n\}.$$

Hence C_1 and C_2 are equivalent.

(ii) Suppose that each of $g_1(x)$ and $g_2(x)$ has an irreducible factor of degree $k-1$ over F_q. Let $g_1(x) = (x-1)\prod_{j=1}^{k-1}(x - \eta^{q^j})$ and $g_2(x) = (x-1)\prod_{j=1}^{k-1}(x - \eta^{iq^j})$, $1 < i < n$, where η is a primitive nth root of unity. Put $s = (n, i)$, $n = sn'$. If $s > 1$, then $g_2(x)$ divides $(x-1)(x^{n'} - 1)$, giving a contradiction for $k \geq 4$. When $k = 3$ we obtain $q \equiv 4t - 1 \bmod n = 8t$ for some integer t (see [12]). Suppose $s > 1$. If i is even, then $g_2(x)$ divides $x^{4t} - 1$, a contradiction. If i is odd, then s divides t and $g_2(x)$ divides $x^{8t'} - 1$, $t = st'$, a contradiction again. Hence $s = 1$ for $k \geq 3$. The remainder is similar with the case (i). □

Let C be a pseudo-cyclic $[n, k]_q$-code with the check polynomial $g(x)$. Assume that $g(x)$ is splitting as $g(x) = \prod_{i=1}^{k}(x - \eta_i)$, $\eta_i \in K$, where K is some extension field of F_q. Then C is MDS if

$$\det \begin{pmatrix} \eta_1^{i_1} & \eta_1^{i_2} & \dots & \eta_1^{i_k} \\ \eta_2^{i_1} & \eta_2^{i_2} & \dots & \eta_2^{i_k} \\ \vdots & \vdots & \ddots & \vdots \\ \eta_k^{i_1} & \eta_k^{i_2} & \dots & \eta_k^{i_k} \end{pmatrix} \neq 0 \qquad \text{for any distinct } i_1, \dots, i_k \text{ with } 1 \leq i_j \leq n.$$

The converse is also true if $g(x)$ is irreducible over F_q.

THEOREM 2.10. *Let C be a pseudo-cyclic $[n, k]_q$-code with the check polynomial $g(x)$. Assume that $g(x)$ is irreducible over F_q, i.e., $g(x) = \prod_{i=1}^{k}(x - \eta^{q^i})$ for some $\eta \in K = F_{q^k}$. Then C is MDS iff $\det(\eta^{i_j q^\ell})_{1 \leq j, \ell \leq k} \neq 0$ for any distinct $i_1, \dots, i_k$ with $1 \leq i_j \leq n$.*

PROOF. Suppose that C is MDS and that $\det S_k = 0$ for some distinct $i_1, \dots, i_k$ with $1 \leq i_j \leq n$, where

$$S_t = \begin{pmatrix} \eta^{i_1} & \eta^{i_2} & \dots & \eta^{i_t} \\ \eta^{i_1 q} & \eta^{i_2 q} & \dots & \eta^{i_t q} \\ \vdots & \vdots & & \vdots \\ \eta^{i_1 q^{t-1}} & \eta^{i_2 q^{t-1}} & \dots & \eta^{i_t q^{t-1}} \end{pmatrix}, \qquad 1 \leq t \leq k.$$

Replacing i_k with other i_j if necessary, there exists $(a_{i_1}^{(k-1)}, \dots, a_{i_{k-1}}^{(k-1)}) \in K^{k-1} \setminus (0, \dots, 0)$ with

$$\sum_{j=1}^{k-1} a_{i_j}^{(k-1)} \eta^{i_j q^\ell} = \eta^{i_k q^\ell} \qquad \text{for } \ell = 0, 1, \dots, k-1.$$

Raising to the qth power, we obtain

$$\sum_{j=1}^{k-1} (a_{i_j}^{(k-1)})^q \eta^{i_j q^\ell} = \eta^{i_k q^\ell} \qquad \text{for } \ell = 0, 1, \dots, k-1.$$

Hence $\det S_{k-1} = 0$ or $a_{i_j}^{(k-1)} \in F_q$, $j = 1, \dots, k-1$. If $\det S_{k-1} = 0$, then we similarly get $\det S_{k-2} = 0$ or $a_{i_j}^{(k-2)} \in F_q$, $j = 1, \dots, k-1$, and so on.

On the other hand, we have $\det S_2 = \eta^{i_1(q+1)}(\eta^{i_2 - i_1} - \eta^{(i_2 - i_1)q}) \neq 0$. Indeed, if $\eta^{i_2 - i_1} \in F_q$, then $g(x)$ divides $x^{i_2 - i_1} - \beta$ for some $\beta \in F_q$, a contradiction. It follows that

$\det S_t \neq 0$ and $a_{i_j}^{(t)} \in F_q$, $1 \leq j \leq t$, for some t $(2 \leq t \leq k-1)$.

Hence $C^\perp$ has a non-zero codeword with weight at most k, giving a contradiction.

The converse is trivial. □

We denote by $m(k, q)$ the maximum value of n for which there exists an $[n, k]_q$-MDS code. It is well known that $m(3, q) = q + 1$ if q is odd, and $m(3, q) = q + 2$ if q is even [6, 10], but there exists no pseudo-cyclic $[q + 2, 3]_q$-MDS code for even q [11, 15]. We have also known that $m(k, q) = q + 1$ for $q \geq k$, $k = 3, 4$ [7, 8]. On the other hand, there exists a $[q + 1, k]_q$-MDS code for any $q \geq k$ by Theorem A. Hence our research of n for which a pseudo-cyclic $[n, k]_q$-MDS code exists is restricted by the following theorem for $k = 3, 4, 5$.

THEOREM C. *The maximum value of n for which there exists a pseudo-cyclic $[n, k]_q$-MDS code is $q + 1$ for $k = 3, 4, 5$.*

LEMMA 2.11. *If $q = p^h \equiv m \bmod n$ $(1 \le m < n-1)$ with $m = p^\ell$ for some ℓ, $1 \le \ell < h$, then no cyclic $[n,k]_q$-MDS code exists for $k = 3, 4, 5$.*

PROOF. Let C be a cyclic $[n, n-k]_q$-MDS code with the generator polynomial $g(x)$. Suppose $q = p^h \equiv m \bmod n$ $(1 \le m < n-1)$ with $m = p^\ell$ for some ℓ, $1 \le \ell < h$. Since $g(\eta) = 0$ implies $g(\eta^q) = g(\eta^{p^\ell}) = 0$, we have $g(x) \in F_{p^\ell}[x]$. On the other hand, any k columns of a parity check matrix $[{}^tP, {}^t(PT), {}^t(PT^2), \ldots, {}^t(PT^{n-1})]$ of C must be linearly independent, where $P = (1, 0, \ldots, 0)$ and T is the companion matrix of $g(x)$. Hence the $[n,k]_{p^\ell}$-code with the check polynomial $g(x)$ is MDS. By Theorem C we obtain $n \le p^\ell + 1 < n$, a contradiction. □

As we see later (in Notes 1 and 4), the only possible cases when there exist no cyclic but pseudo-cyclic $[n,k]_q$-MDS codes for $3 \le k \le 5$ are (i) $k = (n, q-1) = 3$ with $n | q^2+q+1$ and (ii) $k = (n, q-1) = 5$ with $n | q^4+q^3+q^2+q+1$. Corollary 2.6 and Lemma 2.11 induce the following.

COROLLARY 2.12. *Let C be a pseudo-cyclic $[n, n-k]_q$-code with the generator polynomial irreducible over F_q for $k = 3$ or 5. If $(n, q-1) = k$ and if $q = p^h \equiv m \bmod n$ $(1 \le m < n/k - 1)$ with $m = p^\ell$ for some ℓ, $1 \le \ell < h$, then C is not MDS.*

PROOF. Let C be a pseudo-cyclic $[n, n-k]_q$-MDS code satisfying the conditions of Corollary 2.12. Put $n = ks$. Since n divides $\sum_{i=0}^{k-1} q^i$, we have $s \ge 7$ for $k = 3$ and $s \ge 11$ for $k = 5$, and $(s, q-1) = 1$. Hence, by Lemmas 2.1 and 2.3, there exists a cyclic $[s, n-k]_q$-MDS code with $q \equiv p^\ell \bmod s$, $1 \le p^\ell < s-1$, which is contradictory to Lemma 2.11. □

3. PSEUDO-CYCLIC MDS CODES OF DIMENSION THREE (MARUTA [12, 13])

We survey known results on the existence of pseudo-cyclic MDS codes of dimension three, whose proofs are given in [12, 13].

THEOREM 3.1. *Let C be a pseudo-cyclic $[n, 3]_q$-MDS code. Then C must satisfy one of the following conditions:*

(*i*) $8 | n$, $q \equiv n/2 - 1 \bmod n$, $n/2 \ne p^\ell + 1$ $(1 \le \ell < h)$,
(*ii*) $n | q^2+q+1$, $n < q-1$.

The converse is also true except for finitely many primes p.

THEOREM 3.2. *Let t and m be positive integers $(2 \le m < n-1)$. If n and q satisfy the following (i) or (ii), then there exists a pseudo-cyclic $[n, 3]_q$-MDS code except for finitely many primes p:*

(*i*) $n = 8t$, $q \equiv 4t - 1 \bmod n$, $p^\ell \ne 4t - 1$ $(1 \le \ell < h)$,
(*ii*) $n | m^2 + m + 1$, $q \equiv m \bmod n$.

NOTE 1. For a pseudo-cyclic $[n, 3]_q$-MDS code C with the check polynomial $g(x)$, (i) is the case when $g(x)$ has an irreducible factor of degree two over F_q, and (ii) is the case when $g(x)$ is irreducible over F_q. Since $(q-1, q^2+q+1) = 1$ or 3, there exists a cyclic code which is equivalent to C iff $(n, q-1) \ne 3$. For given n, q satisfying the above (i) or (ii), cyclic $[n, 3]_q$-MDS codes are unique up to equivalence by Theorem 2.9. The uniqueness of pseudo-cyclic $[n, 3]_q$-MDS codes satisfying (ii) with $3 | n$ has been proved using a geometric method [17]. See also [14].

THEOREM 3.3. *For $t \le 7$ and q satisfying $q = p^h \equiv 4t - 1 \bmod 8t$, there exists a cyclic $[8t, 3]_q$-MDS code except for the cases:*

(1) $p = 4t - 1$ *for* $t = 1, 2, 3$,
(2) $p = 47, 79$ *for* $t = 4$,
(3) $p = 19, 59$ *for* $t = 5$,
(4) $p = 23, 71, 263$ *for* $t = 6$,
(5) $p = 3, 83$ *for* $t = 7$.

THEOREM 3.4. *There exists a pseudo-cyclic* $[n, 3]_q$*-MDS code,* $q = p^h$, *with*

(1) $n = 7$, $q \equiv 2, 4 \bmod 7$, $p \neq 2$,
(2) $n = 13$, $q \equiv 3, 9 \bmod 13$, $p \neq 3$,
(3) $n = 19$, $q \equiv 7, 11 \bmod 19$, $p \neq 7, 11$,
(4) $n = 21$, $q \equiv 4, 16 \bmod 21$, $p \neq 2$.

4. Pseudo-Cyclic MDS Codes of Dimension Four

LEMMA 4.1. *Let* C *be a pseudo-cyclic* $[n, 4]_q$*-MDS code with the check polynomial* $g(x)$. *If* $g(x)$ *is irreducible over* F_q, *then*

(1) $4|n$ *implies* $q \equiv 1 \bmod 4$,
(2) *there exists no integer* $r > 2$ *with* $r|(n, q + 1)$ *and* $(r, q - 1) = 1$.

PROOF. Let $g(x)$ be the check polynomial of C with $g(x)|x^n - \alpha$, $\alpha \in F_q^*$.

(1) By Corollary 2.6, $4|n$ implies $(q - 1, 4) = 2$ or 4. Suppose $4|n$ and $(q - 1, 4) = 2$. Note that -1 is not a quadratic residue in F_q. Clearly C is not MDS if α is a quadratic residue. If α is not a quadratic residue, there exists $\beta \in F_q$ with $\beta^2 = -\alpha$. Let $n = 4s$. If 2β is a quadratic residue, we have $x^n - \alpha = (x^{2s} + \gamma x^s + \beta)(x^{2s} - \gamma x^s + \beta)$, where $\gamma \in F_q$ with $\gamma^2 = 2\beta$. It implies that $C^\perp$ contains a codeword with weight 3 and hence C is not MDS. Similarly we can deduce that for the case when -2β is a quadratic residue.
(2) Suppose $n = rs, r > 2$ with $r|(n, q + 1)$ and $(r, q - 1) = 1$. Then we have $\rho \in F_{q^2}$ of order r and $\beta \in F_q$ with $\beta^r = \alpha$. Hence $x^n - \alpha = \prod_{i=1}^{r}(x^s - \beta\rho^i)$. Taking $\eta \in F_{q^4}$ with $g(\eta) = 0$, we have $\eta^s = \beta\rho^j$ for some j, $1 \leq j \leq r$. Put $f(x) = (x^s - \beta\rho^j)(x^s - \beta\rho^{jq})$. Then $g(x)$ divides $f(x) \in F_q[x]$ and $f(x) \neq x^n - \alpha$ by $r > 2$. We have $1 < \mathrm{wt}(f(x)) \leq 3$, where $\mathrm{wt}(f(x))$ stands for the weight of a codeword in $C^\perp$ corresponding to $f(x)$, and hence C is not MDS. □

THEOREM 4.2. *Let* C *be a pseudo-cyclic* $[n, 4]_q$*-MDS code. Then* C *must satisfy one of the following conditions:*

(*i*) $q^2 + q + 1 \equiv 0 \bmod n$, $(n, q - 1) = 1$,
(*ii*) $q^2 \equiv -1 \bmod n$, n *odd.*

PROOF. Let $g(x)$ be the check polynomial of C with $g(x)|x^n - \alpha$, $\alpha \in F_q^*$. Suppose that $g(x)$ consists of two irreducible factors of degree two over F_q. By Lemmas 2.4, 2.5 and the Assumption, we have $n/2 = (n, q + 1)$ and $4|n$. Since no pseudo-cyclic $[n/2, 4]_q$-MDS code exists by Theorem A, we get a contradiction. Hence $g(x)$ must be irreducible over F_q or $g(x)$ must have an irreducible factor of degree three over F_q. If $g(x)$ has an irreducible factor of degree three over F_q, then (i) must be satisfied by Corollary 2.7. Suppose that $g(x)$ is irreducible over F_q. By Corollary 2.6, n divides $q^3 + q^2 + q + 1 = (q + 1)(q^2 + 1)$. If q is even, then n must be odd and $(q + 1, q - 1) = 1$. By Lemma 4.1(2), $n|q^2 + 1$ must be satisfied. If q is odd, we have $(q + 1, q - 1) = (q + 1, q^2 + 1) = 2$. From Lemma 4.1(2), there exists no prime $\ell > 2$ dividing $(n, q + 1)$. Hence $(n, q + 1) = 2^s$ for some s (≥ 0). By Lemma 4.1(1) we get $s \leq 1$. Suppose $s = 1$ and $4|n$. Put $n = 2m$. Then m is even and

divides q^2+1. Since α is a quadratic residue in F_{q^2}, Theorem A implies that there exists no α-cyclic $[m,4]$-MDS code over F_{q^2} and hence over F_q. Therefore we have either $s=1$ with $n \equiv 2 \bmod 4$ or $s=0$, which induces $n \mid q^2+1$. If n is even, we can also get a contradiction setting $m=n$ as the above m. Hence (ii) must be satisfied. □

NOTE 2. The condition of the above (ii) implies $(n, q-1)=1$ since $(q-1, q^2+1) \leq 2$. Thus, pseudo-cyclic $[n,4]_q$-MDS codes satisfying the above (i) or (ii) are equivalent with cyclic ones by Lemma 2.1 and hence they are unique up to equivalence by Theorem 2.9.

Can we really construct cyclic $[n,4]_q$-MDS codes when (i) or (ii) of Theorem 4.2 is satisfied? We give an answer of this question for $n=13$ below.

THEOREM 4.3. *If $n=13$ divides q^2+q+1, then there exists a cyclic $[13,4]_q$-MDS code, $q=p^h$, iff $p \neq 2,3$.*

PROOF. Note that $13 \mid q^2+q+1$ implies $q \equiv 3$ or $9 \bmod 13$. Assume $p \neq 2,3$. Let C be a cyclic $[13,4]_q$-code with the check polynomial $g(x)$. Since $(q^2-1, 13)=1$ and $q \equiv 3$ or $9 \bmod 13$, $g(x)=(x-1)(x-\eta)(x-\eta^3)(x-\eta^9)$ for some $\eta \in F_{q^3}$. We assume that η is a primitive nth root of unity. C is MDS if all the matrices

$$S=\begin{pmatrix} 1 & 1 & 1 & 1 \\ \eta^t & \eta^u & \eta^v & \eta^w \\ \eta^{3t} & \eta^{3u} & \eta^{3v} & \eta^{3w} \\ \eta^{9t} & \eta^{9u} & \eta^{9v} & \eta^{9w} \end{pmatrix}, \qquad 1 \leq t < u < v < w \leq 13,$$

are non-singular. Put $f(i,j,k)=\det S$ where $i=u-t$, $j=v-t$ and $k=w-t$. We must see $f(i,j,k) \neq 0$ for $\binom{12}{3}=220$ (i,j,k)'s, $1 \leq i < j < k < 13$. But by the cyclicity and $f(qi,qj,qk)=f(i,j,k)^q$, it is sufficient to investigate $f(i,j,k) \neq 0$ for $(i,j,k)=(1,2,3)$, $(1,2,4)$, $(1,2,5)$, $(1,2,6)$, $(1,2,7)$, $(1,2,8)$, $(1,2,9)$, $(1,2,10)$, $(1,2,11)$, $(1,3,4)$, $(1,3,5)$, $(1,3,7)$, $(1,3,8)$, $(1,3,9)$, $(1,4,6)$, $(1,5,7)$, $(1,5,11)$, $(1,6,8)$, $(1,8,10)$. $f(1,2,3)$ is of Vandermode type and hence $f(1,2,3) \neq 0$. Since $\eta^{13}=1$, $f(i,j,k)$ is calculated to be of degree at most 12. Let $H(x) \in \mathbb{Z}[x]$ with $H(\eta)=f(1,2,4)$. Then $H(\eta^2)=-f(1,2,8)$, $H(\eta^4)=f(1,2,11)$, $H(\eta^7)=f(1,2,7)$. Since $n=13$ is prime, $f(1,2,4) \neq 0$ iff $f(1,2,8) \neq 0$ and so on, say $(1,2,4) \sim (1,2,8) \sim (1,2,11) \sim (1,2,7)$. We also get $(1,2,5) \sim (1,2,10) \sim (1,3,8) \sim (1,5,7)$, $(1,2,6) \sim (1,2,9) \sim (1,3,5) \sim (1,3,7)$, $(1,3,4) \sim (1,6,8)$, $(1,3,9) \sim (1,4,6) \sim (1,5,11) \sim (1,8,10)$. Hence we need to see $f(i,j,k) \neq 0$ only for $(i,j,k)=(1,2,4)$, $(1,2,5)$, $(1,2,6)$, $(1,3,4)$, $(1,4,6)$. Let $G(x)=(x^{13}-1)/(x-1)$. We show $(G,H)=1$ by the euclidean algorithm. Since $q \equiv 3$ or $9 \bmod 13$ we have $p \not\equiv 1,5,8,12 \bmod 13$. We suppose $p \notin \{2,3,7,11\}$. Then we can calculate R_i, $1 \leq i \leq 8$ as follows:

$$\begin{aligned}
&R_1=2G+H,\ R_2=-2H-(x-1)R_1,\ R_3=R_1-(4x+12)R_2,\\
&R_4=\{5\cdot 11^2 R_2-(11x-45)R_3\}/(-4),\\
&R_5=\{7^2\cdot R_3-(5\cdot 7\cdot 11x+5\cdot 13\cdot 31)R_4\}/11^2,\\
&R_6=\{-3^2\cdot 13^4 R_4+(3\cdot 7\cdot 13^2-5\cdot 19\cdot 167)R_5\}/(5\cdot 7^2),\\
&R_7=\{1429^2 R_5-(3\cdot 13^2\cdot 1429x-2\cdot 347771)R_6\}/(3^4\cdot 13^4),\\
&R_8=\{5^2\cdot 7^2\cdot 13^2 R_6-(5\cdot 7\cdot 13\cdot 1429x-3\cdot 17\cdot 47^2)R_7\}/1429^2.
\end{aligned}$$

And we have $R(R_7,R_8)=3^3\cdot 5^8\cdot 7^8\cdot 13^8$, where $R(R_7,R_8)$ stands for the resultant of R_7 and R_8.

When $p=7$, R_i $(1 \leq i \leq 4)$ are as above and

$$R_5=-R_3+(x^2+x)R_4,\ R_6=R_4+(x+5)R_5,\ R_7=\{-R_5+(x^2-2x+2)R_6\}/2,$$

and $R(R_6, R_7) = 3 \neq 0$.

When p=11, $R_i (1 \leq i \leq 3)$ are as above and

$$R_4 = 5R_2 - (x^2 - 2x - 7)R_3,\ R_5 = -2R_3 + (5x - 10)R_4,$$
$$R_6 = R_4 - (x - 1)R_5,\ R_7 = 3R_5 - (x + 2)R_6,$$

and $R(R_6, R_7) = 3 \neq 0$.

It follows that $f(1, 2, 4) \neq 0$ if $p \neq 2, 3$. Similarly we can also prove $f(i, j, k) \neq 0$ for $(i, j, k) = (1, 2, 5), (1, 2, 6), (1, 3, 4), (1, 4, 6)$ if $p \neq 2, 3$, whence there exists a cyclic $[13, 4]_q$-MDS code if $p \neq 2, 3$.

If $p = 3$, then there exists no cyclic $[13, 4]_q$-MDS code by Lemma 2.11.

Assume $p = 2$. Since the multiplicative order of 2 mod 13 is 12, $p^h \equiv 3$ mod 13 iff $4|h$. Hence $g(x) \in F_{16}[x]$. We may assume $q = 16$. Let $g(x) = x^4 - ax^3 - bx^2 - cx - d$ and let T be the companion matrix of $g(x)$ and $P = (1, 0, 0, 0)$. By Theorem 8 in Chapter 11 of [10] and by Theorem A any square submatrix of $[{}^t(PT^4), {}^t(PT^5), \ldots, {}^t(PT^{12})]$ is non-singular if C is MDS. Note that $PT^5 = (ad, ac + d, ab + c, a^2 + b)$ and $n = q - \sqrt{q} + 1$. Now $g(x)$ can be written as follows:

$$g(x) = (x + 1)(x^3 + \gamma x^2 + \gamma^{\sqrt{q}} x + 1),\ \gamma = \eta + \eta^q + \eta^{q^2},$$

where η is a primitive nth root of unity. Hence

$$ac + d = (\gamma + 1)^{\sqrt{q}+1} + 1 = \sum_{i=0}^{12} \eta^i = 0,$$

which implies that there exists no cyclic $[13, 4]_{16}$-MDS code. □

CONJECTURE. Let $6 \leq n \leq q - 2$, $q = p^h$. There exists a pseudo-cyclic $[n, 4]_q$-MDS code iff $n | m^2 + m + 1$, $q \equiv m$ mod n, $p^\ell \neq m$ $(1 \leq \ell < h, 2 \leq m < n - 1)$ and $n \neq q - \sqrt{q} + 1$, $n \not\equiv 0$ mod 3.

NOTE 3. There exists no cyclic $[q - \sqrt{q} + 1, 4]_q$-MDS code for $q = 7^2$. Indeed, for $n = q - \sqrt{q} + 1$, the check polynomial $g(x)$ can be written as $g(x) = (x-1)(x^3 - \gamma x^2 + \gamma^{\sqrt{q}} x - 1)$, $\gamma = \eta + \eta^q + \eta^{q^2}$, where η is a primitive nth root of unity. Let $F_{49} = F_7[\sigma]$, $\sigma^2 + \sigma + 3 = 0$. Put $f_i = x^3 - \sigma^i x^2 + \sigma^{7i} x - 1$. Then $x^{43} - 1 = (x-1) f_3 f_4 f_{10} f_{11} f_{19} f_{20} f_{21} f_{22} f_{25} f_{28} f_{29} f_{31} f_{37} f_{44}$. Let $g_i(x) = (x-1) f_i = x^4 - ax^3 - bx^2 - cx - d$. Note that $\langle g_i(x) \rangle$ and $\langle g_{\sqrt{q}i}(x) \rangle$ are equivalent, where $\langle g_i(x) \rangle$ stands for the code corresponding the ideal of $F_q[x]/(x^n - 1)$ generated by $g_i(x)$. For i=3, $ac + d = 0$. For i=4,20 we have $b = 0$. Let $P_j = PT^j$, where T is the companion matrix of $g(x)$ and $P = (1, 0, 0, 0)$. For $i = 10$ we have $P_{18} = (\sigma^{31}, 0, \sigma^5, \sigma^{18})$. For i =11, $[{}^t P_5, {}^t P_6]$ has a singular submatrix. For i =19, $[{}^t P_{20}, {}^t P_{26}]$ has a singular submatrix. Finally for i =25, $[{}^t P_{22}, {}^t P_{23}]$ has a singular submatrix. Hence there exists no cyclic $[43, 4]_{49}$-MDS code.

Similarly we can also prove the non-existence of cyclic $[q - \sqrt{q} + 1, 4]_q$-MDS codes for $q = 9^2, 13^2$.

THEOREM 4.4. *If $n = 13$ divides $q^2 + 1$, then there exists a cyclic $[13, 4]_q$-MDS code, $q = p^h$, iff $p \neq 2, 5$.*

PROOF. By Lemma 2.11 we may assume $p \neq 2, 5$. Let C be a cyclic $[13, 4]_q$-code with the check polynomial $g(x)$. Since $(q^4 - 1, 13)$=1 and $q \equiv 5$ or 8 mod 13, $g(x) = (x - \eta)(x - \eta^q)(x - \eta^{q^2})(x - \eta^{q^3})$ for some $\eta \in F_{q^4}$, where η is a primitive nth root of unity. C is MDS iff all the matrices

$$S = \begin{pmatrix} \eta^t & \eta^u & \eta^v & \eta^w \\ \eta^{-t} & \eta^{-u} & \eta^{-v} & \eta^{-w} \\ \eta^{5t} & \eta^{5u} & \eta^{5v} & \eta^{5w} \\ \eta^{-5t} & \eta^{-5u} & \eta^{-5v} & \eta^{-5w} \end{pmatrix}, \qquad 1 \leq t < u < v < w \leq 13,$$

are non-singular by Theorem 2.10. Put $i = 2(u-t)$, $j = 2(v-t)$ and $k = 2(w-t)$.

Then

$$\det S = \eta^{i+j}(\eta^i - 1)(\eta^j - 1)(\eta^k - 1)(\eta^i - \eta^j)(\eta^j - \eta^k)(\eta^k - \eta^i) f(i,j,k),$$

where $f(i,j,k) = (\eta^i + \eta^j + \eta^k)(\eta^k + \eta^{k-i} + \eta^{k-j} + 1) + \eta^{k-i} + \eta^{k-j} + 1$.

Clearly, $f(i,j,k)^q = f(iq, jq, kq)$ and $f(i,j,k) = f(k-j, k-i, k)$. Hence it is sufficient to prove that $f(i,j,k) \neq 0$ for $(i,j,k) = (1,2,3), (1,2,4), (1,2,5), (1,2,8), (1,3,4), (1,3,5), (1,3,7), (1,3,9), (1,4,7), (1,4,10), (1,5,7), (1,6,8), (1,7,8), (3,5,7), (4,5,10), (4,7,10)$. By a similar argument with that in the proof of Theorem 4.3, we obtain $(1,2,3) \sim (1,7,8) \sim (4,7,10)$, $(1,2,4) \sim (1,2,8) \sim (1,4,7)$, $(1,2,5) \sim (1,5,7) \sim (3,5,7)$, $(1,3,5) \sim (1,3,7) \sim (4,5,10)$, $(1,3,4) \sim (1,4,10) \sim (1,6,8)$. Calculating $f(i,j,k)$, we get $f(x) \in \mathbb{Z}[x]$ with $f(\eta) = f(i,j,k)$ for each (i,j,k). Put $G(x) = (x^{13}-1)/(x-1)$.

For $(i,j,k) = (1,2,3)$, $\det S \neq 0$, for S is of Vandermode type.

For $(i,j,k) = (1,2,4)$, $R(f, G - (x^4 - x^2)f) = 13 \cdot 53 \cdot 79 \neq 0$.
For $(i,j,k) = (1,2,5)$, $R(f, G - x^2 f) = -1$.
For $(i,j,k) = (1,3,5)$, $R(f, G - x^2 f) = 5^4$.
For $(i,j,k) = (1,3,9)$, $f - G = 2x^9$.
For $(i,j,k) = (1,6,8)$, $R(f, G - x^2 f) = 5^4$.

Hence $f(i,j,k) \neq 0$ for $1 \leq i < j < k \leq 12$ if $p \neq 2, 5$, completing the proof. □

Similarly we can prove the following:

THEOREM 4.5. *There exists a cyclic $[n,4]_q$-MDS code, $q = p^h$, with*

(1) $n = 17$, $q \equiv \pm 4 \bmod 17$, $p \neq 2, 13$,
(2) $n = 25$, $q \equiv \pm 7 \bmod 25$, $p \neq 7, 13$.

PROOF. $17 | q^2 + 1$ implies $q \equiv \pm 4 \bmod 17$, and $25 | q^2 + 1$ implies $q \equiv \pm 7 \bmod 25$. Since our proof is quite similar to that of Theorem 4.4, we omit it here. □

5. Pseudo-Cyclic MDS Codes of Dimension Five

LEMMA 5.1. *Let C be a cyclic $[n,5]_q$-MDS code with the check polynomial $g(x)$. If $g(x)$ has two irreducible factors of degree two over F_q, then $(n, q-1) = 2$.*

PROOF. Let $(n, q-1) = r$ and $n = rs$. By Lemmas 2.4, 2.5(2) and Assumption, we get $r = 2$ or 3. Suppose $r = 3$. Then we have $q \equiv s-1 \bmod 3s$ with $3 | s+1$ or $q \equiv 2s-1 \bmod 3s$ with $3 | s-1$. Let ω be an element of F_q with $\omega^2 + \omega + 1 = 0$. If $q \equiv s-1 \bmod 3s$, then $x^s - \omega^i$ is written as $x^s - \omega^i = (x - \omega^{2i}) \prod_a (x^2 - a\omega^{2i} + \omega^i)$. Putting $f_a(x) = \prod_{i=1}^{3} (x^2 - a\omega^i + \omega^{2i})$ we get $\mathrm{wt}((x^3-1)f_a) \leq 4$. Hence $g(x)$ divides $(x-1) f_a f_b$ for some $a \neq b$ in F_q, which is also true for the case $q \equiv 2s-1 \bmod 3s$. Hence we may assume $g(x) = (x-1)(x - \omega\eta)(x - \omega\eta^{-1})(x - \omega^2\eta^e)(x - \omega^2\eta^{-e})$, $e \not\equiv 0, \pm 1 \bmod s$, where η is a primitive sth root of unity. Let $H = [{}^t P_1, \ldots, {}^t P_n]$, where $P_i = (1, \omega^i \eta^i, \omega^i \eta^{-i}, \omega^{2i} \eta^{ei}, \omega^{2i} \eta^{-ei})$, $i = 1, 2, \ldots, n$. Then every square submatrix of H of size 5 must be non-singular if C is MDS. However, $P_n + a_1 P_{s+1} + P_{2s+2} + a_2 P_1 + a_3 P_{2s+1} = 0$ if $3 | s+1$, and $P_n + a_1 P_{2s+1} + P_{s+2} + a_2 P_1 + P_{s+1} = 0$ if $3 | s-1$, where

$$a_1, a_2, a_3 \in F_q \text{ with } \begin{pmatrix} 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = - \begin{pmatrix} \eta^e + \eta^{-e} \\ \eta + \eta^{-1} \\ 2 \end{pmatrix}.$$

Hence $C^\perp$ has a non-zero codeword with weight at most 5, giving a contradiction. Therefore we obtain $r = 2$. □

THEOREM 5.2. *Let C be a pseudo-cyclic $[n, 5]_q$-MDS code, $q = p^h$. Then C must satisfy one of the following conditions:*

(i) $q \equiv 4t - 1 \bmod n = 8t$ *for some integer* t, $p^\ell \not\equiv 4t - 1$ $(1 \le \ell < h)$,
(ii) $n | m^2 + 1$, $q \equiv m \bmod n$ *with* $p^\ell \not\equiv m$ $(1 \le \ell < h)$, n *odd*,
(iii) $q^4 + q^3 + q^2 + q + 1 \equiv 0 \bmod n$.

PROOF. Let $g(x)$ be the check polynomial of C with $g(x) | x^n - \alpha$, $\alpha \in F_q^*$. If $g(x)$ has a linear factor and an irreducible factor of degree 2 over F_q, then (i) holds by Lemmas 2.5(2), 2.8 and 5.1. If $g(x)$ is irreducible over F_q, then (iii) holds by Corollary 2.6. It follows from Lemma 2.5 that $g(x)$ cannot have an irreducible factor of degree 3 over F_q. Finally we assume that $g(x)$ has an irreducible factor of degree 4 and prove (ii). Lemma 2.5(2) implies that $n | (q+1)(q^2+1)$ and $(n, q-1) = 1$, hence n is odd. We may assume $\alpha = 1$ by Lemma 2.1. Let $(n, q+1) = r$ and $n = rs$. Then there exists $\rho \in F_{q^2}$ with $x^n - 1 = \prod_{i=1}^{r} (x^s - \rho^i)$. Suppose $r > 3$. Then $f(x) = (x^s - 1)(x^s - \rho^j)(x^s - \rho^{jq}) \neq x^n - 1$, where $\rho^j = \xi^s$ and ξ is an element of F_{q^4} with $g(\xi) = 0$. Clearly each coefficient of $f(x)$ is in F_q. Since $g(x)$ divides $f(x)$ and $\mathrm{wt}(f(x)) \le 4$, C cannot be MDS, a contradiction. Hence $r = 3$ if $r > 1$. Suppose $r = 3$. Let η be a primitive sth root of unity and let $x^n - 1 = \prod_{i=1}^{3} (x^s - \omega^i)$, $\omega \in F_q$ with $\omega^2 + \omega + 1$. We may assume $g(\xi) = 0$, $\xi = \omega\eta$. Then $g(x) = (x-1)(x-\omega\eta)(x-\omega\eta^{-1})(x-\omega^2\eta^q)(x-\omega^2\eta^{-q})$. Now calculating a_1, a_2 and a_3 in the proof of Lemma 5.1 for this $g(x)$, we get $a_1 = -(b+b^q+2)/3$, $a_2 = (\omega(b+b^q-4) - b + 2b^q - 2)/3(2\omega+1)$ and $a_3 = (\omega(b+b^q-4) - b^q + 2b - 2)/3(2\omega+1)$, where $b = \eta + \eta^{-1}$. We can easily verify that a_1, a_2 and a_3 are in F_q, giving a contradiction. Therefore $r = 1$ and then n divides $q^2 + 1$. $q \equiv m \bmod n$ implies $p^l \not\equiv m$ $(1 \le \ell < h)$ by Lemma 2.11. □

NOTE 4. Let C be a pseudo-cyclic $[n, 5]_q$-MDS code with the check polynomial $g(x)$. If (i) or (ii) of Theorem 5.2 holds, then C is equivalent to cyclic one by Lemma 2.1. For the case when (iii) of Theorem 5.2 holds, C is equivalent to cyclic one iff $(n, q-1) \neq 5$, since $(q - 1, q^4 + q^3 + q^2 + q + 1) = 1$ or 5. Hence, for given n, q satisfying the above (ii), pseudo-cyclic $[n, 5]_q$-MDS codes are unique up to equivalence by Theorem 2.9, which is also true in the case satisfying (iii) if $(n, q-1) \neq 5$. The smallest possible n and q for which there exist no cyclic but pseudo-cyclic $[n, 5]_q$-MDS codes is the case $n = 55$, $q = 71$.

THEOREM 5.3. *There exists a cyclic $[n, 5]_q$-MDS code, $q = p^h$, with*

(1) $n = 16$, $q \equiv 7 \bmod 16$, $p \neq 7, 23, 71$,
(2) $n = 13$, $q \equiv 5, 8 \bmod 13$, $p \neq 2, 5$,
(3) $n = 11$, $q \equiv 3, 4, 5, 9 \bmod 11$, $p \neq 2, 3, 5$.

The above (1), (2), (3) correspond to (i), (ii), (iii) of Theorem 5.2 respectively. The existence of a cyclic $[8, 5]_q$-MDS code for $q \equiv 3 \bmod 8$, $p \neq 3$, follows from Theorem 3.3(1) by the duality.

PROOF. (Sketch) (1) Let $q = p^h \equiv 4t - 1 \bmod n = 8t$. Since $n | q^2 - 1$ and

$$x^{8t} - 1 = (x^{4t} + 1)(x^{2t} + 1)(x^t + 1)(x^t - 1),$$

we may assume that $g(x) = (x-1)g_1(x)g_2(x)$, $g_1(x) | x^{4t} + 1$, $g_2(x) | x^{2t} + 1$, so that $g_1(x)$ and $g_2(x)$ are irreducible polynomials over F_q of degree two. (Note that $\langle g(x) \rangle$ cannot be MDS if $(g(x), x^t + 1) \neq 1$.)

Let η be a root of $g_1(x)$. The other root of $g_1(x)$ is $\eta^q = -\eta^{-1}$. Since $g_2(x)$ has $\eta^{2(2\ell-1)}$ as a root for some integer ℓ, $\langle g(x) \rangle$ is MDS if any five of n-set

$$\{(1, \eta^i, (-\eta^{-1})^i, \eta^{2i(2\ell-1)}, \eta^{-2i(2\ell-1)}); i = 1, 2, \ldots, n\}$$

TABLE 1.
Existence of pseudo-cyclic $[n, 3]_q$-MDS codes, $q \leq 64$.

$n\backslash q$	5	7	8	9	11	13	16	17	19	23	25	27	29	31	32	37	41	43	47	49	53	59	61	64
5	C	N	N	C	C	N	C	N	C	N	C	N	C	C	N	N	C	N	N	C	N	C	C	C
6	C	C	N	N	C	C	N	C	C	C	C	N	C	C	N	C	C	C	C	C	C	C	C	N
7		C	C	C	C	C	N	N	N	C	C	C	C	N	N	C	C	C	N	C	C	N	N	C
8		C	N	C	C	N	N	C	C	C	C	N	N	C	N	N	C	C	C	C	N	C	N	N
9			C	N	N	N	N	C	C	N	N	N	N	N	N	C	N	N	N	N	C	N	N	C
10				C	C	N	N	N	C	N	N	N	C	C	N	N	C	N	N	C	N	C	C	N
11					C	N	N	N	N	C	N	N	N	N	C	N	N	C	N	N	N	N	N	N
12					C	C	N	N	N	C	C	N	N	N	N	C	N	N	C	C	N	C	C	N
13						C	C	N	N	N	C	C	C	N	N	N	N	N	N	N	C	N	C	C
14						C	N	N	N	N	N	C	C	N	N	N	C	C	N	N	N	N	N	N
15							C	N	N	N	N	N	C	C	N	N	N	N	N	N	N	C	C	N
16							N	C	N	C	N	N	N	C	N	N	N	N	C	C	N	N	N	N
17							C	C	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
18								C	C	N	N	N	N	N	N	C	N	N	N	N	C	N	N	N
19									C	N	N	N	N	N	N	C	N	N	N	C	N	N	N	C
20									C	N	N	N	N	N	N	N	C	N	N	N	N	C	C	N
21										N	S	N	N	N	N	S	C	C	N	N	N	N	N	C
22										C	N	N	N	N	N	N	N	C	N	N	N	N	N	N
23										C	N	N	N	N	N	N	N	N	C	N	N	N	N	N
24										C	C	N	N	N	N	N	N	N	C	C	N	C	N	N
25											N	N	N	N	N	N	N	N	N	C	N	N	N	N
26											C	C	N	N	N	N	N	N	N	N	C	N	N	N
27												N	N	N	N	N	N	N	N	N	C	N	N	N
28												C	C	N	N	N	N	N	N	N	N	N	N	N
29													C	N	N	N	N	N	N	N	N	C	N	N
30													C	C	N	N	N	N	N	N	N	C	C	N
31														C	C	N	N	N	N	N	N	N	C	N
32														C	N	N	N	N	N	N	N	N	N	N
33															C	N	N	N	N	N	N	N	N	N
34																N	N	N	N	N	N	N	N	N
35																N	N	N	N	N	N	N	N	N
36																C	N	N	N	N	N	N	N	N
37																C	N	N	?	N	N	N	N	N
38																C	N	N	N	N	N	N	N	N
39																	N	N	N	N	N	N	N	N
40																	C	N	N	N	N	N	N	N
41																	C	N	N	N	N	N	N	N
42																	C	C	N	N	N	N	N	N
43																		C	N	C	N	N	N	N
44																		C	N	N	N	N	N	N
45																			N	N	N	N	N	N
46																			C	N	N	N	N	N
47																			C	N	N	N	N	N
48																			C	C	N	N	N	N
49																				N	N	N	N	N
50																				C	N	N	N	N
51																					N	N	N	N
52																					C	N	N	N
53																					C	N	N	N
54																					C	N	N	N
55																						N	N	N
56																						N	N	N
57																						N	N	S
58																						C	N	N
59																						C	N	N
60																						C	C	N
61																							C	N
62																							C	N
63																								C
64																								N
65																								C

TABLE 2.
Existence of pseudo-cyclic $[n, 4]_q$-MDS codes, $q \leq 64$.

$n\backslash q$	5	7	8	9	11	13	16	17	19	23	25	27	29	31	32	37	41	43	47	49	53	59	61	64
6	S	C	N	N	S	C	N	S	C	S	C	N	S	C	N	C	S	C	S	C	S	S	C	N
7		C	C	C	C	C	N	N	N	C	C	C	C	N	N	C	C	C	N	C	C	N	N	C
8		S	N	C	N	N	N	C	N	S	C	N	N	S	N	N	C	N	S	C	N	N	N	N
9			C	N	N	N	N	C	C	N	N	N	N	N	N	C	N	N	N	N	C	N	N	C
10				S	C	N	N	N	S	N	N	N	S	C	N	N	C	N	N	S	N	S	C	N
11					C	N	N	N	N	C	N	N	N	N	C	N	N	C	N	N	N	N	N	N
12					S	C	N	N	N	S	C	N	N	N	N	C	N	N	S	C	N	S	C	N
13						C	N	N	N	N	C	C	C	C	N	N	N	N	C	N	C	N	C	C
14						S	N	N	N	N	N	S	C	N	N	N	S	C	N	N	N	N	N	N
15							C	N	N	N	N	N	C	C	N	N	N	N	N	N	N	C	C	N
16							N	C	N	N	N	N	N	S	N	N	N	N	S	C	N	N	N	N
17							C	C	N	N	N	N	N	N	N	N	N	N	C	N	N	N	N	N
18								S	C	N	N	N	N	N	N	C	N	N	N	N	S	N	N	N
19									C	N	N	N	N	N	N	C	N	N	N	N	N	N	N	?
20									S	N	N	N	N	N	N	N	C	N	N	N	N	S	C	N
21										N	N	N	N	N	N	N	C	C	N	N	N	N	N	C
22										C	N	N	N	N	N	N	N	S	N	N	N	N	N	N
23										C	N	N	N	N	N	N	N	N	C	N	N	N	N	N
24										S	C	N	N	N	N	N	N	N	S	C	N	N	N	N
25											N	N	N	N	C	N	N	N	N	C	N	N	N	N
26											S	C	N	N	N	N	N	N	N	N	C	N	N	N
27												N	N	N	N	N	N	N	N	N	C	N	N	N
28												S	C	N	N	N	N	N	N	N	N	N	N	N
29													C	N	N	N	?	N	N	N	N	C	N	N
30													S	C	N	N	N	N	N	N	N	S	C	N
31														C	C	N	N	N	N	N	N	N	C	N
32														S	N	N	N	N	N	N	N	N	N	N
33															C	N	N	N	N	N	N	N	N	N
34																N	N	N	N	N	N	N	N	N
35																N	N	N	N	N	N	N	N	N
36																C	N	N	N	N	N	N	N	N
37																C	N	?	?	N	N	N	N	N
38																S	N	N	N	N	N	N	N	N
39																	N	N	N	N	N	N	N	N
40																	C	N	N	N	N	N	N	N
41																	C	N	N	N	N	N	N	N
42																	S	C	N	N	N	N	N	N
43																		C	N	N	N	N	N	N
44																		S	N	N	N	N	N	N
45																			N	N	N	N	N	N
46																			C	N	N	N	N	N
47																			C	N	N	N	N	N
48																			S	C	N	N	N	N
49																				N	N	N	N	N
50																				S	N	N	N	N
51																					N	N	N	N
52																					C	N	N	N
53																					C	N	N	N
54																					S	N	N	N
55																						N	N	N
56																						N	N	N
57																						N	N	N
58																						C	N	N
59																						C	N	N
60																						S	C	N
61																							C	N
62																							S	N
63																								C
64																								N
65																								C

TABLE 3.
Existence of pseudo-cyclic $[n, 5]_q$-MDS codes, $q \leq 64$.

$n\backslash q$	7	8	9	11	13	16	17	19	23	25	27	29	31	32	37	41	43	47	49	53	59	61	64
7	C	C	N	N	C	N	N	N	N	N	C	C	N	N	N	C	C	N	C	N	N	N	C
8	C	N	C	C	N	N	C	C	C	C	N	N	C	N	N	C	C	C	C	N	C	N	N
9		C	N	N	N	N	C	C	N	N	N	N	N	N	C	N	N	N	N	C	N	N	C
10			C	C	N	N	N	C	N	N	N	C	C	N	N	C	N	N	C	N	C	C	N
11				C	N	N	N	N	C	N	N	N	C	C	C	N	C	C	C	C	C	N	N
12				C	C	N	N	N	C	C	N	N	N	N	C	N	N	C	C	N	C	C	N
13					C	N	N	N	N	C	C	N	C	N	N	N	N	C	N	C	N	N	C
14					C	N	N	N	N	N	C	C	N	N	N	C	C	N	N	N	N	N	N
15						C	N	N	N	N	N	C	C	N	N	N	N	N	N	N	C	C	N
16						N	C	N	N	N	N	N	C	N	N	N	N	C	C	N	N	N	N
17						C	C	N	N	N	N	N	N	N	N	N	N	?	N	N	N	N	N
18							C	C	N	N	N	N	N	N	C	N	N	N	N	C	N	N	N
19								C	N	N	N	N	N	N	C	N	N	N	N	N	N	N	N
20								C	N	N	N	N	N	N	N	C	N	N	N	N	C	C	N
21									N	N	N	N	N	N	N	C	C	N	N	N	N	N	C
22									C	N	N	N	N	N	N	N	C	N	N	N	N	N	N
23									C	N	N	N	N	N	N	N	N	C	N	N	N	N	N
24									C	C	N	N	N	N	N	N	N	C	C	N	?	N	N
25										N	N	N	N	?	N	N	?	N	C	N	N	N	N
26										C	C	N	N	N	N	N	N	N	N	C	N	N	N
27											N	N	N	N	N	N	N	N	N	C	N	N	N
28											C	C	N	N	N	N	N	N	N	N	N	N	N
29												C	N	N	N	?	N	N	N	C	N	N	N
30												C	C	N	N	N	N	N	N	C	C	N	N
31													C	C	N	N	N	?	N	N	N	C	N
32													C	N	N	N	N	?	N	N	N	N	N
33														C	N	N	N	N	N	N	N	N	N
34															N	N	N	N	N	N	N	N	N
35															N	N	N	N	N	N	N	N	N
36															C	N	N	N	N	N	N	N	N
37															C	N	?	N	N	N	N	N	N
38															C	N	N	N	N	N	N	N	N
39																N	N	N	N	N	N	N	N
40																C	N	N	N	N	?	N	N
41																C	N	N	N	N	?	N	N
42																C	C	N	N	N	N	N	N
43																	C	N	N	N	N	N	N
44																	C	N	N	N	N	N	N
45																		N	N	N	N	N	N
46																		C	N	N	N	N	N
47																		C	N	N	N	N	N
48																		C	C	N	N	N	N
49																			N	N	N	N	N
50																			C	N	N	N	N
51																				N	N	N	N
52																				C	N	N	N
53																				C	N	N	N
54																				C	N	N	N
55																					N	N	N
56																					N	N	N
57																					N	N	N
58																					C	N	N
59																					C	N	N
60																					C	C	N
61																						C	N
62																						C	N
63																							C
64																							N
65																							C

are linearly independent.

Now, setting $t = 2$, there exists a cyclic $[16, 5]_q$-MDS code if any five of K_i are linearly independent for $i = 1$ or 2, where

$$K_1 = \{(1, \eta^i, \eta^{2i}, (-\eta^3)^i, \eta^{4i}); i = 1, 2, \ldots, 16\},$$
$$K_2 = \{(1, (-\eta)^i, (-\eta^2)^i, \eta^{3i}, \eta^{4i}); i = 1, 2, \ldots, 16\}.$$

By tedious calculation, it can be deduced that K_1 gives an MDS code if $p \notin \{7, 23, 71, 167, 311\}$ and that K_2 gives an MDS code if $p \notin \{7, 23, 71, 103, 151, 439\}$. (Calculate the determinant of a matrix consisting of each 5-subset of K_i, say f, and calculate the resultant of f and $\eta^8 + 1$). Hence there exists a cyclic $[16, 5]_q$-MDS code if $p \notin \{7, 23, 71\}$. Conversely it is easily checked that every cyclic $[16, 5]_q$-code is not MDS if $p \in \{7, 23, 71\}$.

(2) and (3) can be proved similarly to proofs of Theorems 4.3 and 4.4 using the euclidean algorithm. □

6. Tables

In this final section we give a survey on the existence problem for pseudo-cyclic $[n, k]_q$-MDS codes with $q \leq 64$ for $k = 3, 4, 5$, which are based on results in the previous sections. In the tables, C means the existence of a cyclic $[n, k]_q$-MDS code; S means the existence of a pseudo-cyclic $[n, k]_q$-MDS code and the non-existence of a cyclic $[n, k]_q$-MDS code; and N means the non-existence of a pseudo-cyclic $[n, k]_q$-MDS code. Blank cells stand for 'N' from Theorem C. We can find 'S' for $k = 3, n = 21, 57$, but not for $k = 5$ in our tables.

References

1. E. F. Assmus, Jr and H. F. Mattson, Jr, New 5-designs, *J. Comb. Theory*, **6** (1969), 122–151.
2. E. R. Berlekamp, *Algebraic Coding Theory,* McGraw-Hill, New York, 1968.
3. G. Falkner, W. Heise, B. Kowol, and E. Zehendner, On the existence of cyclic optimal codes, *Atti Semin. Mat. Fis. Univ. Modena*, **28** (1979), 326–341.
4. J. Georgiades, Further results on cyclic MDS-codes, *Atti Semin. Mat. Fis. Univ. Modena*, **32** (1983), 248-254.
5. J. Georgiades, Zyklische MDS-Codes, Dissertation, Technischen Universität München, 1983.
6. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Clarendon Press, Oxford, 1979.
7. J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions,* Oxford University Press, Oxford, 1985.
8. J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries,* Oxford University Press, Oxford, 1991.
9. A. Krishna and D. V. Sarwate, Pseudocyclic maximum-distance-separable codes, *IEEE Trans. Inf. Theory* , **36** (1990), 880–884.
10. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.
11. T. Maruta, A geometric approach to semi-cyclic codes, in: J. W. P. Hirschfeld *et al.* (eds), *Advances in Finite Geometries and Designs*, Oxford University Press, Oxford, 1991, pp. 311–318.
12. T. Maruta, On the existence of pseudo-cyclic MDS codes of dimension three, *Atti Semin. Mat. Fis. Univ. Modena*, **XLI** (1993), 457–471.
13. T. Maruta, Cyclic and pseudo-cyclic MDS codes of dimension three, *Atti Semin. Mat. Fis. Univ. Modena*, **XLIII** (1995), 529–533.
14. T. Maruta, Cyclic arcs and pseudo-cyclic MDS codes, *Discrete Math.*, to appear.
15. Jens P. Pedersen and Carsten Dahl, Classification of pseudo-cyclic MDS codes, *IEEE Trans. Inf. Theory* , **37** (1991), 365–370.

16. V. C. Rocha Jr, Maximum distance separable multilevel codes, *IEEE Trans. Inf. Theory* , **30** (1984), 547–548.
17. L. Storme and H. Van Maldeghem, Cyclic arcs in $PG(2, q)$, *J. Algebr. Comb.*, **3** (1994), 113–128.

Received 12 October 1993 and accepted 21 July 1997

T. MARUTA
Aichi Prefectural University,
Mizuho,
Nagoya 467,
Japan
E-mail: QAJ65715@biglobe.ne.jp